AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Northern District of New York

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

A UMX MOBILE PHONE, MODEL U693CL, CURRENTLY LOCATED AT THE UNITED STATES PROBATION OFFICE FOR THE NORTHERN DISTRICT OF NEW YORK IN SYRACUSE, NEW YORK, AS DESCRIBED IN ATTACHMENT A

Case No. 5:21-MJ-73 (ML)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

A UMX MOBILE PHONE, MODEL U693CL, CURRENTLY LOCATED AT THE UNITED STATES PROBATION OFFICE FOR THE NORTHERN DISTRICT OF NEW YORK IN SYRACUSE, NEW YORK, AS DESCRIBED IN ATTACHMENT A

located in the Northern District of New York, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252A(a)(2)(A)	Knowingly receiving or distributing any child pornography through any means of interstate commerce, including by computer; Knowingly possessing or accessing, with intent to view, any material containing an image of child pornography that has been transported through interstate commerce, including by computer.
18 U.S.C. § 2252A(a)(5)(B)	

The application is based on these facts:

See attached affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Martin Baranski
Applicant's signature

Special Agent Martin Baranski
Printed name and title

ATTESTED TO BY THE APPLICANT IN ACCORDANCE WITH RULE 4.1 OF THE FEDERAL RULES OF CRIMINAL PROCEDURE

Date: February 1, 2021

Miroslav Lovric
Judge's signature

City and state: Binghamton, NY

Hon. Miroslav Lovric, United States Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF A UMX MOBILE PHONE MODEL U693CL, CURRENTLY LOCATED AT THE UNITED STATES PROBATION OFFICE FOR THE NORTHERN DISTRICT OF NEW YORK IN SYRACUSE, NEW YORK AND FURTHER DESCRIBED IN ATTACHMENT A	Case No. 5:21-MJ-73 (ML)

AFFIDAVIT IN SUPPORT OF AN
APPLICATION FOR A SEARCH WARRANT

I, Martin Baranski, being first duly sworn, hereby depose and state as follows:

Introduction

1. I am a special agent employed by the United States Department of Justice, Federal Bureau of Investigation (FBI). As such, I am an "investigative or law enforcement officer" of the United States empowered by law to conduct investigations and make arrests for offenses enumerated in Title 18, United States Code, Chapter 63. I have been a Special Agent with the FBI since October of 2018. I am currently assigned to the FBI's Albany Division where I investigate all federal criminal violations. I have participated in investigations of people suspected of violating federal child pornography laws, including Title 18, United States Code, Section 2252A. I have received training in child sexual exploitation investigations and have had the opportunity to observe and review examples of child pornography in all forms of media including computer media. I also have participated in the application for and execution of several federal search warrants in child sexual exploitation and child pornography investigations.

2. I am currently investigating Thomas Sczerbaniewicz for knowingly receiving, possessing, and accessing with intent to view child pornography, in violation of 18 U.S.C.

§ 2252A(a)(2)(A) and (a)(5)(B) (the "Subject Offenses"). This affidavit is submitted in support of an application for a search warrant to search a UMX mobile phone Model # U693CL (the "Device"), more fully described in Attachment A.

3. The warrant requested here would authorize the forensic examination of the Device for the purpose of identifying electronically stored data more particularly described in Attachment B.

4. The statements and facts set forth in this affidavit are based in significant part on information provided to me from the United States Probation Office and my personal training and experience. Because this affidavit is being submitted for the limited purpose of securing a search warrant for the Device, I have not included every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the Subject Offenses are presently located on the Device.

Probable Cause

5. In December 2009, United States District Court Judge David N. Hurd sentenced Sczerbaniewicz principally to 72 months' imprisonment and lifetime supervised release following Sczerbaniewicz's guilty plea to plea to two counts of receipt of child pornography and one count of possession of child pornography, in violation of 18 U.S.C. § 2252A(a)(2)(B), (a)(2)(A) and (a)(5)(B). Included among the conditions of supervised release is the following condition concerning computer use, monitoring, and searches:

> The defendant shall not use or possess any computer or any other device with online capabilities, at any location, except at his or her place of employment, unless the defendant participates in the Computer Restriction and Monitoring Program. The defendant shall permit the United States Probation Office to conduct periodic, unannounced examinations of any computer equipment the

> defendant uses or possesses, limited to all hardware and software related to online use (e.g., use of the World Wide Web, e-mail, instant messaging, etc.). These examinations may include retrieval and copying of data related to online use, and the viewing of pictures and movies which may be potential violations of the terms and conditions of supervised release from this computer equipment including any internal or external peripherals, internet-capable devices, and data storage media. This computer equipment may be removed to the Probation Office or to the office of their designee for a more thorough examination. The Probation Office may use and/or install any hardware or software system that is needed to monitor the defendant's computer use, subject to the limitations described above.

6. Sczerbaniewicz began his term of supervised release in April 2014. On January 28, 2021, the United States Probation Office was contacted by an employee of New Step, Sczerbaniewicz's sex offender treatment provider. The New Step employee advised the Probation Office that Sczerbaniewicz had been in a bathroom stall for approximately four hours. When the employee asked what Sczerbaniewicz was doing, Sczerbaniewicz said that he was "looking stuff up." The employee was concerned about the amount of time Sczerbaniewicz was in the stall and his comment that he was looking stuff up.

7. Based on the information provided by the New Step employee, the Probation Office went to Sczerbaniewicz's residence in the afternoon of January 28, 2021 to interview him and seize and search any electronic devices that he might have used to access the internet.

8. Sczerbaniewicz admitted to the Probation Office that he was in the bathroom stall at New Step looking at "naughty images" on the Device, that he had been doing so for the last few months, and that he had deleted his browser history. Sczerbaniewicz also turned the Device over

to the Probation Office.[1] Based on information received from New Step, it appears that Sczerbaniewicz was able to access an open WiFi connection from the bathroom.[2]

9. In or about the morning of January 29, 2021, based on the search authority in Sczerbaniewicz's special conditions of supervised release, the Probation Office extracted data from the Device as part of its supervision (*i.e.*, not for the purpose of conducting a thorough examination of the Device for evidence of the Subject Offenses as described in Attachment B). Among other material on the Device, the Probation Office saw thumbnail images consistent with child erotica and child pornography, including thumbnail images of prepubescent boys and girls displaying their genitals in a lewd and lascivious manner.

10. In total, there were over twenty thumbnail images on the Device that were consistent with child pornography, as well as dozens more consistent with child erotica. Your affiant has reviewed those thumbnail images consistent with child pornography, including:

a. .thumbdata4—1967290299_embedded_454.jpg – depicts an approximately 8 year old female child, fully nude, sitting down with her legs spread, using her hand to spread her vagina open[3]

Definitions and Technical Terms

11. The following definitions apply to this affidavit and Attachments A-B:

---

[1] When Sczerbaniewicz acquired the Device in September 2020 he told the Probation Office. He was instructed at that time that he could not use the Device's WiFi capability to access the internet.

[2] New Step's WiFi is password protected, but a different, unprotected WiFi source apparently reaches the bathroom area of New Step's space.

[3] This image is available to the Court for review upon request.

a. "Child erotica" means materials or other items that are sexually arousing to persons having a sexual interest or desire in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or body positions.

b. "Child pornography" includes any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (b) the visual depiction was a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. See 18 U.S.C. § 2256(8).

c. "Computer" refers to an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." See 18 U.S.C. § 1030(e)(1).

d. "Computer-related documentation" consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.

e. "Computer software" is digital information that can be interpreted by a computer and any of its related components to direct the way it works. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

f. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices

(including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware.

g. "Minor" means any person under the age of 18 years. 18 U.S.C. § 2256(1).

h. "Sexually explicit conduct" applies to the visual depictions that involve the use of a minor, see 18 U.S.C. § 2256(8)(A), or that have been created, adapted, or modified to appear to depict an identifiable minor, see 18 U.S.C. § 2256(8)(C). In those contexts, the term refers to actual or simulated: (a) sexual intercourse (including genital-genital, anal-genital, oral-genital, or oral-anal), whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person. See 18 U.S.C. § 2256(2)(A).

i. "Visual depictions" include undeveloped film and videotape, as well as data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. $ 2256(5).

Electronic Storage and Forensic Analysis

12. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period on the device. This information can sometimes be recovered with forensics tools.

13. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes

described on the warrant but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the

computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

14. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

15. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

Conclusion

16. Based on the foregoing, I respectfully submit that there is probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seize the evidence described in Attachment B.

ATTESTED TO BY THE APPLICANT IN ACCORDANCE WITH RULE 4.1 OF THE FEDERAL RULES OF CRIMINAL PROCEDURE

Martin Baranski

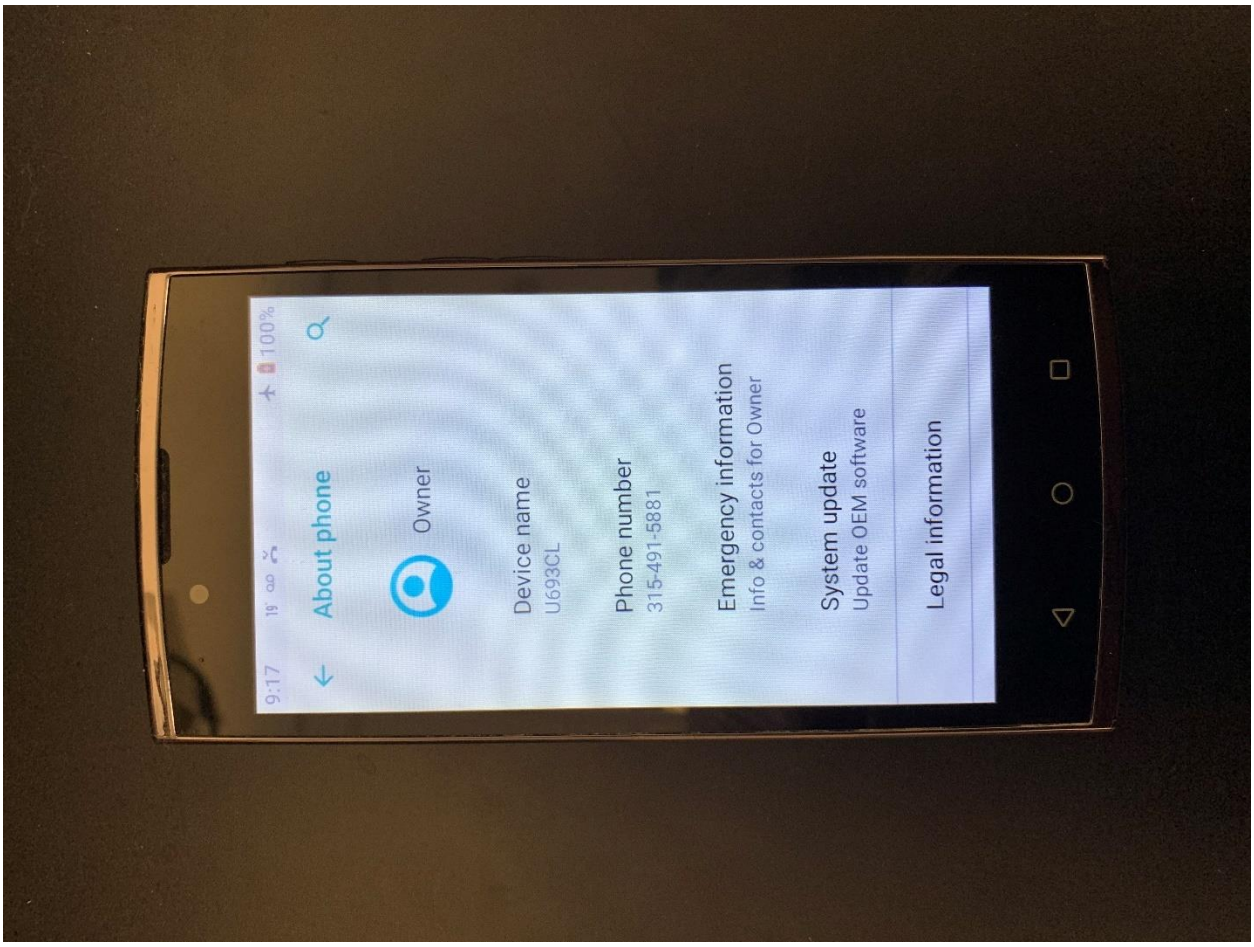
Martin Baranski

I, the Honorable Miroslav Lovric, United States Magistrate Judge, hereby acknowledge that this affidavit was attested to by the affiant by telephone on February 1, 2021, in accordance with Rule 4.1 of the Federal Rules of Criminal Procedure.

Miroslav Lovric
U.S. Magistrate Judge

ATTACHMENT A

The property to be searched is a UMX Mobile Phone Model U693CL, currently located at the United States Probation Office for the Northern District of New York in Syracuse, New York and depicted below:



This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Items and information that constitute fruits, evidence, and instrumentalities of violations of 18 U.S.C. § 2252A(a)(2)(A) and (a)(5)(B) (receipt, possession, and access with intent to view child pornography) described as follows:

1. Visual depictions of minors engaged in sexually explicit conduct as defined in Title 18, United States Code, Section 2256.
2. Evidence of when, how, and in what manner any visual depiction of a minor engaged in sexually explicit conduct came to be on the Device and how and where such visual depiction is/was saved on the Device.
3. Evidence of visits to websites that offer visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256.
4. Evidence identifying people transmitting through interstate or foreign commerce any visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256.
5. Evidence identifying who the user was who created, received, and/or possessed any child pornography found on the Device.
6. Evidence pertaining to the creation, receipt, and/or possession of visual depictions of minors engaged in sexually explicit conduct as defined in Title 18, United States Code, Section 2256, and evidence that would assist in identifying any victims of the above-referenced criminal offenses, including address books, names, and lists of names and addresses of minors, or other information pertinent to identifying any minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2).

7. All child erotica, including photographs of children that are not sexually explicit, images of drawings, images of sketches, fantasy writings, and notes evidencing an interest in unlawful sexual contact with children, and evidence assisting authorities in identifying any such children.
8. Evidence of user attribution for the Device.
9. The authorization includes the search of the electronic media listed on the face of the warrant, for electronic data remnant data, and slack space.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.